

Homeland Defense Journal

"He is best secure from dangers who is on his guard even when he seems safe." —Syrus Publilius

Homeland Defense Journal, Inc. | Suite 1003 | 4301 Wilson Boulevard | Arlington, Virginia 22203
www.homelanddefensejournal.com | Phone: 703-807-2758 | Fax: 703-807-2758

WHAT'S INSIDE

Publisher's Notes	Page 2
Vulnerability of Wireless Local Area Networks to Interception	Page 6
Getting a GSA Schedule Contract	Page 10
The Homeland Security Act: Implications for Government Contractors	Page 12
Verga Clarifies DoD's Homeland Defense Role	Page 15
Homeland Defense Journal to Survey and Profile its Readership	Page 16
Wargame Reveals Port Security Threat	Page 17
Hundreds of Billions Being Spent for War on Terrorism	Page 18
Calendar of Events	Page 19
Bush Orders Smallpox Shots for Military, First Responders	Page 20
Homeland Head, Health Care Pros Outline President's Smallpox Plan	Page 20
DoD Looks Forward to Working With Homeland Security Department	Page 22
Transportation Security Mission Is 'Far From Over,' Agency Head Says	Page 22
Civil Air Patrol and FAA: Drug Trafficking and Terrorism Are Connected	Page 24
Faces In The Crowd	Page 25
Homeland Defense Business Opportunities	Page 25
Business Briefs	Page 26

OUR STAFF

PUBLISHER

Don Dickson
ddickson@homelanddefensejournal.com
301-455-5633

EDITOR

Marianne Dunn
mdunn@homelanddefensejournal.com
703-807-2495

CIRCULATION

David Dickson
dicksond@homelanddefensejournal.com
703-807-2758

REPORTING STAFF

Steve Kingsley
skingsley@homelanddefensejournal.com
703-807-2758

Kelly Kingsley
kkingsley@homelanddefensejournal.com
703-807-2758

George Groesbeck
ggroesbeck@marketaccess.com
941-360-3663

Tony Rahimi
trahimi@homelanddefensejournal.com
703-807-2758

GRAPHIC DESIGN

Dawn Woelfle
dwoelfle@homelanddefensejournal.com
941-746-4923

ADVERTISING AND SPONSOR SALES

Cara Lombardi
clombardi@homelanddefensejournal.com
703-807-2743

Government vs. Private Enterprise: Who Should Control the Airwaves?

By Paul Shultz
For Homeland Defense Journal

At a public meeting Thursday, Nov. 7, 2002, the Federal Communications Commission appeared to resolve a long-running dispute between the U.S. government and the private sector by real-locating some of the airwaves occupied by the Department of Defense to potential commercial advanced wireless services, such as "third-generation" wireless or "3G."

So-called 3G represents the future of today's wireless phones — multimedia devices capable of transmitting and receiving voice, data and video communications around globe.

The FCC's action Nov. 7 is significant because in the wake of the Sept. 11, 2001, terrorist attacks, the DoD insisted that it needed all the radiofrequency (RF) spectrum it was authorized to use for national security purposes. Indirectly, that raised the question of who should control prime spectrum — public or private sector.

After the terrorist attacks, both Congress and the Bush Administration were more than willing to accept DoD's national security argument. Clearly, the immediate post-9/11 reaction was that the military needed to control the airwaves to defend the homeland. Thus, proposals to trans-

fer government spectrum to the private sector were placed on the back burner.

Nobody argued with that decision, despite the fact that Congress, in the early 1990s, had directed the federal government to transfer some 200 megahertz of spectrum to the private sector in exchange for authorizing the FCC to auction the spectrum. This directive was included in the Omnibus Budget Reconciliation Act of 1993.

During the past year, however, discussions between the FCC, which administers the private sector airwaves, and the National Telecommunications and Information Administration

continued on page 3

Gilmore Commission Calls for Independent Center to Coordinate Terrorism Intelligence

A National Counter Terrorism Center should be created to operate as an independent intelligence agency that would coordinate information about potential terrorist attacks in the United States and report directly to the president, a federal commission recommended Monday, Dec. 16, 2002.

In its fourth annual report to President Bush and Congress, the commission — chaired by former Virginia Gov. James S. Gilmore III — recommended that the National Counter Terrorism Center be a separate entity not connected to the FBI, CIA or the Department of Homeland Security.

The formal title of the federally chartered commission, created in 1999 to assess the nation's preparedness for terrorist attacks, is the Advisory Panel to Assess Domestic

Response Capabilities for Terrorism Involving Weapons of Mass Destruction. It is commonly known as the Gilmore Commission.

"The FBI's long standing law enforcement tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be transformed into an organization dedicated to detecting and preventing terrorist attacks," the Gilmore Commission report said. "It is also important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of 'secret police.'"

The commission also recommended that, when the military is used to fight terrorism in the United States, it be clearly relegated to the support of civilian authorities.

continued on page 4

Publisher's Notes

By Don Dickson
Homeland Defense Journal

The Gilmore Commission Report - Wrestling with Issues of Strategic Importance to this Country

We have reported in this issue of **Homeland Defense Journal** on the fourth report by the Gilmore Commission. This commission was activated in 1999 to assess the nation's preparedness for terrorist attacks. The most current set of recommendations was released on Monday, Dec. 16, 2002. Former Governor of Virginia James S. Gilmore III heads this commission and held a press conference on the day of release. I attended this press conference and would like to share my impressions.

The commission is wrestling with issues that have long-term consequences

for this country. How shall we balance our nation's commitment to civil liberties against the realities of embedded terrorists in this country and abroad? What is the appropriate role of the U.S. military in a civil action? How do we prevent internal intelligence gathering from becoming a secret police armed with both intelligence and arrest authority? This commission is appropriately setting the stage for a national dialogue on these and many other issues.

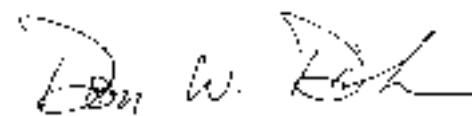
During the hour-long press conference, Gilmore focused on these strategic issues and the position taken by the commission. He quoted Benjamin Franklin who stated, "Those who give up liberty for

the sake of security deserve neither liberty nor security." Franklin wrote these words as part of his *Historical Review of Pennsylvania* in 1759, nearly 30 years before there was a U.S. Constitution. The commission is clearly sensitive to the importance of this national debate and their role in it.

However, there is another dialogue that needs to take place in parallel. More than 50,000 people read each issue of **Homeland Defense Journal**. We hear from and meet with many state and local leaders responsible for infrastructure protection, first response, public health and safety. Just when dollars are most needed to fund these critical local initiatives, our country enters a recession. States, counties, cities and other local governments are fighting just to pay the bills and have little, if any, available for developing their protections and response capabilities. All disasters are local.

The Gilmore commission touched on the funding issue in their report. But there are more questions than answers. Gilmore reported that "the majority of hospitals are private." How then, do we implement a national strategy aimed at improving our surge capabilities for WMD/biological attacks? Farms are commercial enterprises. How do we implement food safety programs? Who will pay the tab ... especially when the tab is getting larger?

We urge the commission, Congress and the national leadership to begin a parallel dialogue on funding sources and strategies for meeting the growing needs at state and local government levels. The needs are well documented. The solution remains elusive.



Don W. Dickson

Safety & Security Solutions

- Interoperable Communications & Information Networks
- Identification & Tracking Systems
- Command & Control Operations
- Physical Security & Monitoring Systems

To Meet Your Needs for Homeland Defense

www.motorola.com/homelandsecurity


MOTOROLA
intelligence everywhere

Mark your calendar !

Regional, State and Local Homeland Defense

Colorado Springs, Colorado
January 14-16, 2003
(Includes special Grants Workshop)

Homeland Defense Outlook 2003

February 6, 2003
Arlington, Virginia

Government Best Practices Training
The GAO Redbook in Practical Terms –
The Rules and Law of Appropriations
Washington, D.C.
February 25 – 26, 2003

Government Best Practices Training Managing Human Capital

Washington, D.C.
February 27, 2003

Homeland Defense: Information Sharing
Arlington, Virginia
February 26, 2003

Homeland Defense: Cyber Infrastructure Protection
Arlington, Virginia
March 11, 2003

For more information on these training conferences, go to
www.homelanddefensejournal.com

Government vs. Private Enterprise: Who Should Control the Airwaves?

continued from page 1

(NTIA), a unit of the U.S. Department of Commerce that oversees federal government spectrum, reached a different conclusion about who should control some of the most sought-after spectrum in the airwaves. Last summer, NTIA released a study showing that 45 megahertz of prime spectrum in the 1.7 GHz band occupied by DoD could be reallocated to commercial services such as 3G.

The NTIA report, *An Assessment of the Viability of Accommodating Advanced Mobile Wireless (3G) Systems in the 1710-1755 MHz and 2110-2170 MHz Bands*, found that the 1710-1755 MHz band could be cleared of government users — at least by December 2008. NTIA also suggested that this spectrum could be auctioned in the 2004-2005 time frame.

The FCC, which is under pressure from private industry to find spectrum for future 3G services, essentially agreed. At the meeting in November, the commission reallocated the 1710-1755 MHz band (along with the 2110-2155 MHz band, which is under its jurisdiction) to advanced wireless services, such as 3G. The FCC also adopted a rulemaking proposal seeking public comment on service and licensing rules for this spectrum.

The commercial wireless industry praised the FCC's decision. The Cellular Telecommunications & Internet Association (CTIA) — the organization that represents most U.S. cellular and personal communications service carriers — said the commission's decision would help the wireless industry bring innovative services to consumers.

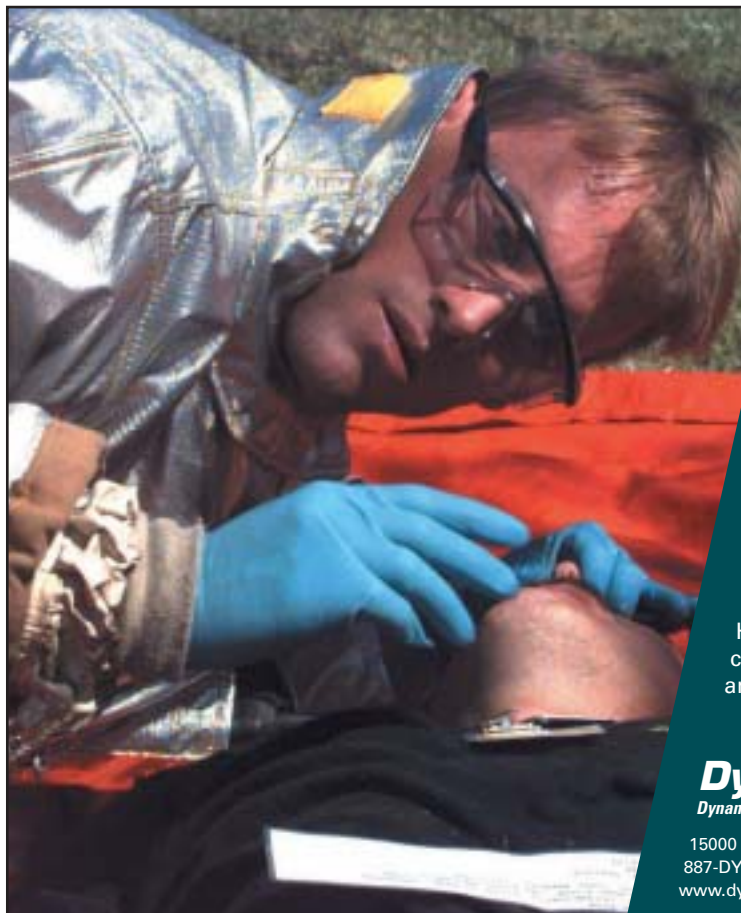
But there are some questions about customer demand for advanced wireless services.

The rollout of second-generation (2G) services, such as digital cellular and PCS, over the past decade resulted in an increase in the number of subscribers to mobile telecommunications service from less than 10 million in 1992 to approximately 140 million today — roughly a 14-fold subscribership increase in a single decade. And cell phone calls from the Sept. 11 victims on hijacked planes and in the World Trade Center seemed to highlight the importance of wireless communications as a safety factor.

This helped fuel the industry's desire to take the mobile handset to the next level and add multimedia features for people "on the go." The average customer, however, has not yet bought into this vision. Various studies have revealed that most people continue to use their mobile phones primarily for voice communications and ignore advanced features such as text messaging and Internet access. In fact, customers overwhelmingly chose to access the Internet via landline offerings, such as digital subscriber line or cable TV modem technology. It might very well be that wireless access could one day catch on but, so far, that has not happened.

Perhaps the best indication of lack of customer demand for 3G is that the major U.S. wireless carriers this year successfully lobbied the U.S. government to postpone auctions for licenses in spectrum earmarked for these advanced services, including the 1.7 GHz band. The recent downturn in the economy, as well as litigation over a previous FCC re-auction of licenses originally granted to NextWave Telecom, contributed to the wireless industry's efforts to delay future 3G spectrum auctions.

continued on page 4



When terror strikes... How will you respond?

Your worst nightmare will become reality hours or even days before you know about it, and the two things you need to respond – time and information – are two things you probably won't have.

DynCorp's Homeland Security Incident Reporting and Tracking System (HIRTS) helps you take back the advantage. HIRTS is the first highly customizable command and control application that combines secure wireless technology, real time incident reporting and pattern recognition with infinite scalability.

Whether used on-site by first responders or in hospitals to monitor for the first signs of a WMD attack, HIRTS combines all available information to create a cohesive, real-time picture of the situation, detect trends and put time back on your side.

DynCorp

Dynamic. Dedicated. Driven.

15000 Conference Center Drive, Chantilly, VA 20151
887-DYN-INFO (396-4636) DSSCustomerRelations@DynCorp.com
www.dyncorp.com

Government vs. Private Enterprise: Who Should Control the Airwaves?

continued from page 3

Arguably, it would seem, the DoD should retain its incumbent rights to the 1.7 GHz spectrum. But NTIA and others have conducted studies showing that the military is extremely inefficient in its use of spectrum and that, more often than not, the frequencies it controls are unused most of the time. This is why Congress determined, nearly a decade ago, that big chunks of government-occupied spectrum should be transferred to the private sector. Still, it is not clear today that private enterprise is any more efficient in its use of the spectrum than the federal government, or that the private sector has an overwhelming need to use more frequencies for services that customers will purchase.

Neither government nor private enterprise makes the best use of the spectrum under their control. In part, this can be blamed on century-old government policy that essentially granted incumbent spectrum rights on a first come, first served basis without much thought to the future, or to where in the spectrum different systems could operate in relation to one another. Hence, the FCC today is faced with messy reallocation problems whenever it decides to reallocate spectrum to new services.

The FCC attempted to address this problem by creating a Spectrum Policy Task Force of senior commission staff that recently released 39 recommendations regarding both policy and technical issues. However, that may be too little too late because the FCC oversees only the private sector spectrum. Despite much-publicized "coordination" efforts, the commission has no control over the government spectrum administered by the NTIA.

Just as President Bush proposed a single, homogenous Homeland Security Department, his administration could consider proposing a single agency to oversee and coordinate both public and private sector spectrum. Such an agency would determine what would best serve the needs of both federal and commercial interests.

Paul Shultz is the communications director for the Washington, D.C., law firm of Blooston, Mordkofsky, Dickens, Duffy & Prendergast.

Gilmore Commission Calls for Independent Center to Coordinate Terrorism Intelligence

continued from page 1

"Coming through this crisis without diminishing our freedoms or our core values of individual liberty is the entire game," Gilmore said. "If we pursue more security at the cost of what makes us Americans, the enemy will have won."

The commission recommended that the National Counter Terrorism Center be staffed with intelligence analysts transferred from the FBI, CIA and other existing agencies.

The National Counter Terrorism Center would be responsible for the fusion of intelligence from all foreign and domestic sources, and be responsible for disseminating information to many "customers." Customers would include federal agencies such as the Departments of Justice, Homeland Security and State; local law enforcement; state officials; and the private sector.

Policy Recommendations

The 19-member Gilmore Commission issued policy recommendations in five key areas:

- **Organizing the National Effort:** In addition to the creation of the National Counter Terrorism Center, the commission recommended more authority for the Department of Homeland Security. This authority would give the Department the power to coordinate the response to bioterrorism attacks and an expanded role in the analysis of intelligence involving protection of the nation's critical infrastructure.
- **Establishing Appropriate Structures, Roles and Missions for the Department of Defense:** Additional changes are needed to ensure an appropriate role for the nation's military and the National Guard in protecting the United States from and responding to terrorist attacks, the commission said. To be effective while ensuring the

protection of civil liberties, military personnel must be trained, equipped, and exercised for potential military operations inside the United States. There must also be better coordination with civil authorities, at all levels, on appropriate military roles.

- **Improving Health and Medical Capabilities:** The commission recognized the Department of Health and Human Services' effort to fund improvements in state and local public health preparedness at record speed after the anthrax attacks, and called for continued funding over five years to strengthen the nation's public health system. American hospitals have improved terrorism planning, but most are unprepared for an attack, the commission found. Preparations are hampered by a lack of federal resources and difficult health care economics that have strained finances of most hospitals.
- **Defending Against Agricultural Terrorism:** The U.S. agriculture industry and food supply appear particularly vulner-

continued on page 6

COOP Consulting

Continuity of Operations Services for Government & Military Clients

- Certified training for continuity of operations planners
- Web-based plan software in partnership with Microsoft
- Certified staff using industry-standard methodology

12096 Kinsley Place, Reston, VA www.coop-consulting.com
Contact: Vicki Ellis at 703-467-0574 or vicki@coop-consulting.com

Women-Owned Small Business

Officers Do Their Best Work On The Streets



Keep Them There

There's no doubt about it: the public is best protected when your officers are in the field. But with a typical mobile data system, their time on the streets is severely compromised by the type of routine communications that are simply too data-intensive to be performed remotely. Alvarion's high-speed mobile data networking solutions can change that. From simple email communications to complex data reporting, Alvarion gives your agents a complete mobile office.

But just as officers on the street must be equipped with protective gear, so must the network they use to send and receive mission-critical communications. You've got to arm your officers and their data. And while most wireless networking systems have poor security, Alvarion has been providing law enforcement agencies with truly secure fixed and mobile wireless networking solutions since 1995. Using Frequency Hopping Spread Spectrum, multiple layers of keys and encryption, and anti-jamming capabilities, our systems perform their security tasks flawlessly – so that your officers can too. Because in this line of work, secure high-speed communications can mean the difference between a mission accomplished and a mission compromised.

High-speed, high-security mobile networking.
Alvarion gives you both.



Gilmore Commission Calls for Independent Center to Coordinate Terrorism Intelligence

continued from page 4

able to terrorism, but actual threats from terrorists need to be defined, the commission found. Several dual-use actions can be taken to protect the agricultural sector and food supply from terrorist attacks and naturally occurring disease outbreaks, including increasing laboratory capacity, education and training to deal with foreign animal diseases.

- **Improving the Protection of Critical Infrastructure:** The Gilmore Commission recommended creation of an independent commission to suggest strategies for protection of the nation's critical infrastructure, and urged that the Department of Homeland Security elevate the priority of other aspects of critical infrastructure protection.

Vulnerability of Wireless Local Area Networks to Interception

By David C. Jenn and
Navy Lt. Paul Sumagaysay
For Homeland Defense Journal

A wide variety of wireless systems are used in both the civilian and military sectors. Many organizations have chosen wireless local area networks (WLANs) over hardwired networks because of their convenience and flexibility. One challenge in deploying systems that radiate in free space is the possibility of the signal being intercepted by unauthorized users. For example, portable computers with client adapter antennas could be placed covertly so as to intercept the WLAN microwave transmission signal.

Even though the power levels involved are very low, a person just outside of a building or in a lobby could conceivably receive and record signals for analysis at a later time. There are unique propagation conditions that occur inside of buildings and in "urban canyons" that could enhance signal detection under certain circumstances. Thus, the WLAN is vulnerable to uninvited intruders who could collect sensitive information or possibly even disrupt the computer network by injecting deceptive signals.

According to K. Pahlavan's article "Trends in Local Wireless Networks," which was published in the March 1995 issue of IEEE Communications Magazine, several security measures have been incorporated into the WLAN standards. For example, authentication and encryption would provide data security. And, networks with media access control (MAC) contain address-based access lists on access points registers and recognize MAC addresses that are allowed to join the network. Radius server-based authentication would provide security for the network by assuring that users are authenticated against a centralized radius server that is based on the MAC address or the username and password.

Encryption between the wireless adapter and the access point would provide security with the network. Wired equivalent privacy is an algorithm designed to provide privacy for data transmitted between the wireless client and the access point. It utilizes data encryption with 40-bit or 128-bit keys that are hidden from users, according to Sandeep Singhal's "The Seven Deadly Sins of Wireless LANS," available at www.reefedge.com.

Although complex encryption techniques would make it difficult for the average person to penetrate the system, the algorithms built into the network software have been defeated by knowledgeable hackers. The first step in the hacking process would be gaining unauthorized access to network traffic. In many cases this is most easily accomplished by intercepting wireless signals. Thus, predicting and subsequently con-

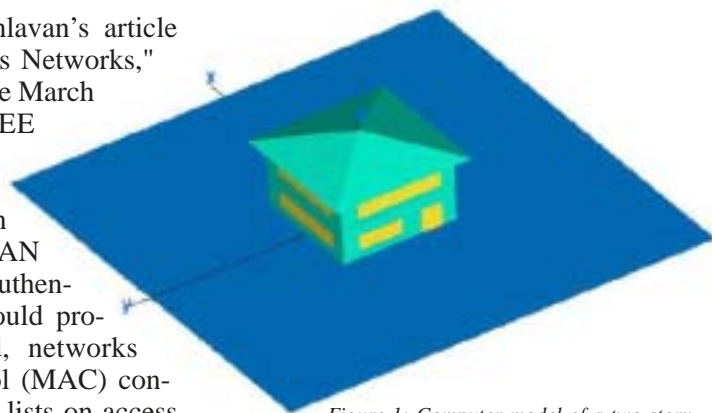


Figure 1: Computer model of a two-story office building

trolling the electromagnetic radiation is an effective means of securing the network.

In general, the approach to providing effective WLAN access for users is to position hubs to cover the desired area adequately, most often by trial and error. Electromagnetic wave propagation modeling in indoor and urban environments is difficult because of the interactions between a large number of scattering objects such as walls and furniture. Modern buildings and furnishings use many materials that affect propagation by attenuation, reflection, and diffraction. Building walls, floors, landscape, and even adjacent buildings affect the manner in which these signals propagate.

The underlying electromagnetic theory is well understood, and accurate propagation simulations are achievable with sufficient computational resources, such as CPU time and memory, and high-fidelity building models. Often, the lack of knowledge of the materials enclosed in a wall limits the accuracy of a simulation, not a shortcoming in the electromagnetic analysis.

continued on page 7

ABOUT COBALT

Cobalt is an Internet application development and hosting firm that specializes in working with mid-sized to large corporations and professional trade associations.

For more information go to
<http://www.cobalt.net/>



Vulnerability of Wireless Local Area Networks to Interception

continued from page 6

Research at the Naval Postgraduate School, sponsored by the Department of Justice, has examined the vulnerability of WLANs to interception and provided some simple steps that can be taken to improve security. Science Application International Corp.'s Urbana Wireless Toolset was used to predict signal levels in complex environments such as the inside of a building. The propagation model is essentially a 3-D ray tracing process that predicts the local mean power received at any given point. The model includes the effects of wave polarization, material properties, and antenna patterns. The simulations provided contours of power levels that could predict the maximum detection distance of the wireless signals.

Figure 1 shows a model of a two-story building that might be occupied by a small business. The building footprint is a square, 40 feet on a side. A WLAN access point antenna, located on the first floor at the + symbol, was considered to

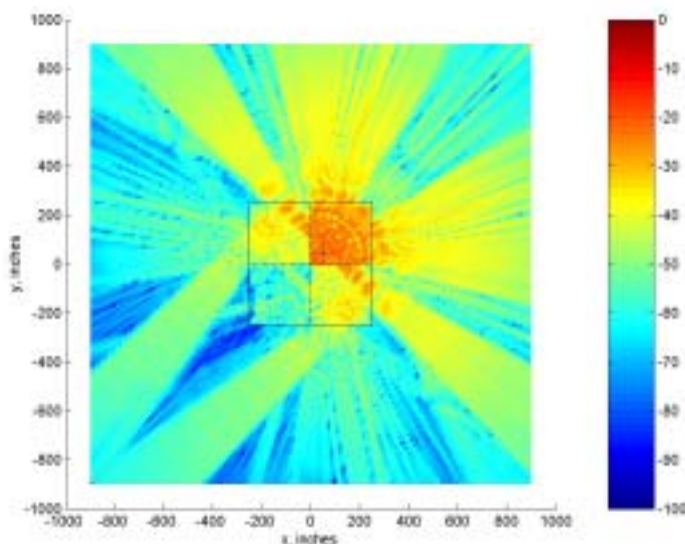


Figure 2: Power levels for a building with metal composite walls and standard glass windows. Units are decibels relative to a milliwatt (dBm). Strong signals passing through the windows are evident.

be transmitting. The signal levels were calculated at points inside and outside of the building using *Urbana*.

Figure 2 shows the power levels for a transmitter power of 100 milliwatts, which is the highest power allowed. The building walls are a metal composite, and standard glass windows are used.

The receiver sensitivity is the minimum power required for maintaining the link. WLAN sensitivities range from -94 dBm for 1 Mbps to -85 dBm for 11 Mbps, where dBm is a decibel relative to a milliwatt reference, according to www.cisco.com. Although the strongest signals are confined to the interior of the building, significant levels are transmitted through the walls and windows. No interception would be possible in the dark blue areas. Note that at the lowest data rate, interception is possible over most of the computational grid that is 1800 inches (150 feet) on a side.

In Figure 3 the standard glass windows are replaced by tinted glass. There has been a significant reduction in the power outside of the building. A further reduction in power can be achieved by moving the transmit antenna to the second floor, as evident in Figure 4.

The fact that the WLAN is contained inside a closed building gives a false

continued on page 8



eye for transport

Cargo Security Forum 2002

Conference • exhibition • workshops

How to manage the impact and cost of cargo security initiatives. . . and still retain a fast, reliable and competitive supply chain

December 4-6, 2002 Georgetown University Conference Center, Washington DC.

The only independent event to focus on real solutions to counter cargo theft and terrorist threats across the global logistics chain

Over three information packed days experts from across the industry and government will provide answers to these burning questions:

- How much will new security initiatives cost and who will end up paying for them?
- Which companies are implementing the best supply chain security programs and how?
- How are the various government agencies working together and collaborating with the trade community to ensure an effective security program?
- Which security technologies and initiatives will provide real return on investment?

Top level speakers include

TSA	Dole
FBI	APL
US Customs	Target Corp.
Exel	CNF
Kraft Foods	Port Authority NY NJ
Roadway Express	KLM Cargo
CSX	and more...

FREE cargo security research paper!

FAX BACK this form to +44 20 7375 7576 or contact Cal Foster on 1800 814 3459 x200 or cal@eyefortransport.com

- ☐ Please send me the Cargo Security Research paper
☐ Please send me more info on the Cargo Security Forum

Full name.....
 email.....
 Company.....
 Phone.....
 Job Title.....

www.eyefortransport.com/cargosecurity

Vulnerability of Wireless Local Area Networks to Interception

continued from page 7

sense of security. Many small businesses use WLANs, yet system administrators are not aware of the susceptibility of these systems to interception, or feel that they do not have the resources to tighten security. However, some steps could reduce the probability of interception, including:

1. locate access points in the most interior building spaces

2. close all exterior doors and windows
3. use metal blinds or tinting on exterior windows
4. use directive or sectorized access point antennas to confine the direction of strong radiation
5. use the lowest possible power settings
6. buildings with metal exterior walls are preferred over those with wood

These simple measures can deny terrorists access to the information they need to inflict damage.

Dr. David C. Jenn is an associate professor in the Department of Electrical & Computer Engineering at the Naval Postgraduate School. Paul Sumagaysay is a lieutenant in the U.S. Navy, and recently graduated from the Information Warfare program at the Naval Postgraduate School.

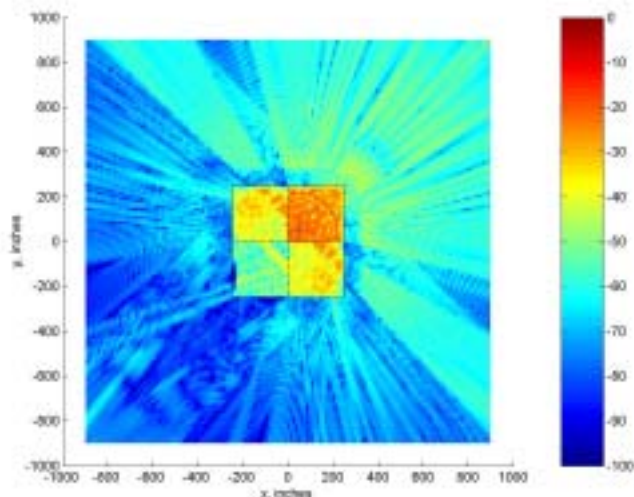


Figure 3: Outside power levels are reduced using tinted glass, which reflects signals back into the building.

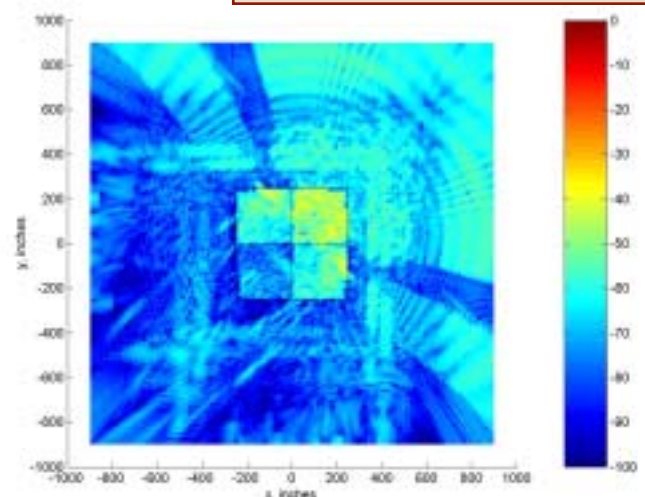


Figure 4: Outside power levels are reduced further after moving the access point antenna to the second floor.

- Functions 24/7 yeararound in any climate.
- Provides warning in time for action.
- A system for today and tomorrow: expandable multi-sensor integration platform.
- Affordable.
- Covers biological and chemical threats by establishing upper and lower control limits.
- Limits false positive and negative responses.
- Robust, reproducible and verifiable.
- Allows for remote operation.

Call today: 218.624.2800
www.apprisetech.com

Looking for a reliable
 solution to your
Early Warning
 needs?
 Look to **RUSS!**
 Water supply
 protection.

Apprise
 technologies, inc.
 Measurement and Control. Accuracy with Ease.

Homeland Defense Grants Report and Grants Database

Grants to support homeland defense

It's a new funding opportunity. Are you ready?

The Bush Administration will use grants as the distribution channel of choice to move billions of dollars to state and local governments. New rules. New policy. New procedures. New funding opportunities.

- **Value to State and Local Governments:** Be sure to take full advantage of all grants opportunities available to your agency
- **Value to product and services contractors:** Your state and local clients will be receiving funds to purchase products and services. Learn what they will be buying, what the rules are and funds available.

What's In The Homeland Defense Journal Grants Report:

U.S. Federal Grants for Homeland Defense

A profile of legislation and agency testimony outlining agency plans for grants to support state and local homeland defense needs. Agency administrators outline their priorities and goals with respect to homeland defense grants.

Audit and Compliance

The Bush Administration will increase oversight, audit and compliance reporting requirements. How to be prepared for an audit. Practical steps to make sure your organization is compliant.

Writing Your Grants Proposal

A practical guide for how to prepare for and write your grants proposal. Lessons-learned and best practices are defined by a company that makes its business writing successful grants proposals.

Grants Opportunities for State and Local Governments

A complete listing of over 160 federal grants to support state and local governments planning, preparations and outfitting for homeland security and defense. Also included are state grants from New York, Texas and selected private grants.

Points of Contact – State and Local Government

Get to know who is responsible for the grants initiative within each state.

The Homeland Defense Journal's Grants Database Includes over 160 Grants from Federal, State, private and regional agencies. Go to www.homelanddefensejournal.com for a sampling.

Order Form

Special Introductory Price Per Copy – Valid to 15 January 2003:

- Federal, state government: \$395.00 (Must have .us, .mil or .gov email address and be a full-time government employee)
- Corporations, Government Support Contractors, Associations: \$595

Distribution will be on, or about 1 January 2003.

Please Print

Name _____

Title _____

Organization _____ Amount Due: \$ _____

Address _____

City/State/Zip _____

Make Check Payable to: Homeland Defense Journal, Inc. Suite 1003, 4301 Wilson Boulevard, Arlington, Va. 22203

Credit Card: ☐ VISA ☐ MC ☐ AMEX

Phone _____ Credit Card # _____

Fax _____ Expiration Date _____

E-Mail _____ Signature _____

FAX COMPLETED FORM TO: 703-807-2728 - All materials in this report are copyrighted and duplication of printed and/or electronic materials is prohibited.

Getting a GSA Schedule Contract

By Hope A. Lane
For Homeland Defense Journal

Slashed corporate budgets, swelling federal government coffers and the creation of the Department of Homeland Security are the three biggest factors compelling commercial companies to embark on federal government sales campaigns.

The federal government is projected to spend more than \$225 billion in fiscal year 2003. A large percentage of these dollars is expected to go to federal contractors, increasing the desire to be among those on the receiving end stronger every day.

Commercial companies have flocked to the government like an oasis of hope in the desert of falling sales. For those looking at the government for the first time, or rethinking previous decisions not to, one of the most widely used types of federal contracts is the General Services Administration's (GSA) Schedule contract. GSA Federal Supply Service manages this program in which contractors are awarded long-term contracts used by buyers within the federal government. The GSA schedules program evolved from years of procurement reform initiatives. The result is a contract that embraces commercial sales practices. Not only can commercial companies use this contract to sell to federal agencies, the contract supports a pro-active sales process that commercially oriented companies are accustomed to.

The more attractive features of GSA Schedule contracts are:

- Prices established based on how much something was sold for rather than how much it cost to produce it
- Eliminates the need for complex cost accounting systems to comply with federal cost-based regulations
- Significantly reduces the time for government orders
- Flexible contract allows teaming and strategic relationships

All of these features contribute to the success of the program and over the last few years these contracts have become the procurement vehicle of choice by many. Total GSA Schedule sales for fiscal year 2002 are \$22 billion dollars, representing a 20 percent increase over total sales for fiscal year 2001. And they are on the rise: Total schedule sales are estimated at \$25 billion for 2003. If you're looking at the federal market, you cannot ignore these numbers.

Companies interested in the emergence of homeland defense spending will be interested in the following GSA Supply Schedule contracts:

- Solutions and more (SAM)
 - Security and guard services
 - Facility security products
 - Law enforcement products
 - Bomb detection equipment
 - Facility hardening products
- In vitro diagnostics, reagents, test kits and test sets
 - Anthrax, smallpox testing kits
 - Biological test kits

- Information Technology
 - Cybersecurity
 - Cybersurveillance
 - Biometrics
- Professional Engineering Services
- Logistics Worldwide
 - Deployment of resources
- Training
- Language Services

You may be wondering if this contract is right for you or how you can get one. It's not easy but don't let the daunting process scare you away.

Following the steps below will help you get started:

1. Do your homework. Attend one of GSA's "How to Obtain a GSA Schedule Contract" workshops. Learn about the schedules program by reading GSA's "Multiple Award Schedules Program Owners Manual." Register for workshops and download the publication at www.pub.fss.gov.
2. Visit GSA's electronic commerce site, www.gsaadvantage.gov, to see if your competitors have schedule contracts, what they are selling and for how much.
3. Decide which schedule best represents the products/services you want to sell. For a listing of GSA Schedule contracts visit www.gsaelibrary.gsa.gov/elib/Schedules
4. Download the selected solicitation from www.fedbizopps.gov.

continued on page 11

Experience www.GrantsOffice.com

Online Database Services

- Compiled Federal, State, & Foundation Grants
- Daily Grant Additions & Updates
- Weekly Grant Email & FAX Notifications
- Easily Customizable Features
- Funding Resource Hyperlinks

**GRANTS
OFFICE**

Phone: 585. 241. 4329
www.grantsoffice.com
info@grantsoffice.com

Empowering Communities

Getting a GSA Schedule Contract

continued from page 10

5. Dedicate the resources to put together a quality offer. The process of getting one of these potentially lucrative contracts is very time consuming. If you don't have qualified and experienced internal resources to dedicate to this project then it may be wise to consider outsourcing the effort.
6. Develop a sound pricing strategy based on your commercial discounting policies or practices. GSA's objective is to negotiate prices that are better than or equal to your best customer under similar terms and conditions. Most professional service companies do not have published commercial price lists and essentially have ad hoc discounting practices. Constructing an effective and supportable pricing strategy in this environment can be tricky.
7. Recognize that the solicitation doesn't tell the whole story about what GSA needs to effectively evaluate your offer. Not knowing or abiding by the unwritten rules can cause significant delays in result in lost profits. Don't throw volumes of data at them; it can end up costing you in the negotiations.

Getting a GSA Schedule is only part of the process. To be successful you must create a marketing plan geared toward the idiosyncrasies of the federal government.

The federal government is the world's largest buyer of goods and services. Doing business with it can be very lucrative,

but breaking in requires a dedicated effort and patience.

Don't consider the government as a single entity, but rather many entities. Initially, select one or two agencies to focus on. Take the time to identify the key people. What are their particular needs? What contracts do they like to use? What is their procurement process and how can you make it easier for them to buy from you?

The answers to all of these questions will change depending on the agency and the procuring office.

Remember, people generally buy from people they know and trust. Face time is just as important in addressing the federal market as any other market. Also, don't overlook the importance of strategic relationships, which are particularly important for new market entrants. Identifying successful federal prime contractors and developing subcontract opportunities is an effective way to gain a toehold in the federal market place. Penetrating the federal market takes time and knowledgeable resources. The initial investment may be more than you realized but the payoffs can be HUGE!

Hope A. Lane is director of GSA Schedule Consulting Services for Rockville, MD-based Aronson & Company, a nationally ranked accounting and consulting firm. Lane manages a team of consultants that assists clients in obtaining GSA Schedule contracts and provides consulting support in the areas of pricing strategy and contract administration. She is a guest speaker and lecturer for associations, industry trade groups and congressional representatives and a featured speaker on GSA schedules at Aronson & Company's Executive Briefings.

Join our Team!!

Homeland Defense Journal

Homeland Defense Journal has an immediate opening for an intern to cover homeland security on Capitol Hill. The successful candidate must have a keen understanding of the government; Hill experience preferable. Candidate must also handle administrative duties.

**Submit resumes via e-mail to the publisher –
ddickson@homelanddefensejournal.com.
Please do not send attachments –
paste resumes in e-mail.**

Good Design is Good Business

Woelfle Graphic Design
- Dawn Woelfle -

5265D Jamestown Circle
Bradenton, Florida 34208
Ph: 941.746.4923
Fax: 425.920.8601
dwnmrie@graphic-designer.com



freelance graphics studio

The Homeland Security Act: Implications for Government Contractors

By Dave Nadler and Bradley Wine
For Homeland Defense Journal

On November 25, 2002, President Bush signed the Homeland Security Act, creating a new Department of Homeland Security and a new set of challenges and opportunities for government contractors. The creation of DHS was the largest reorganization of the federal government in more than 50 years, bringing under one umbrella as many as 22 existing separate agencies, including Immigration and Naturalization Service, Secret Service, Customs Service, Federal Emergency Management Agency and the new Transportation Security Administration.

Charged with centralizing the nation's defenses against future terrorist attacks, DHS was divided into four divisions:

- Border and transportation security
- Emergency preparedness and response
- Countermeasures for nuclear, biological, chemical and radiological attacks
- Intelligence analysis

Former Pennsylvania Gov. Tom Ridge, who has served as Bush's director of domestic security, has been nominated to serve as secretary of the new department.

The Homeland Security Act would bolster the president's efforts to use government contracts, grants and other vehicles to encourage the private sector to develop and implement innovative technologies to enhance homeland security. Industry research firms have forecasted that technology spending for DHS will reach \$2.6 billion in fiscal year 2003 with the following technologies in high demand:

- Bio-hazard detection
- Decontamination equipment and techniques
- Vaccines and antidotes to address biological, chemical, radiological and related threats
- Information technology upgrades and products designed to improve data mining and information sharing
- Cybersecurity
- Biometrics

- Equipment and techniques to secure the nation's shipping, transportation and energy infrastructures

To encourage industry to sell cutting-edge technology to the government, the act contained numerous provisions designed to streamline the procurement process and to protect contractors from possible liability and competitive harm.

Procurement Laws and Regulations

As an executive department, DHS would be subject to current procurement laws and regulations. At the same time, the new agency would be permitted to deviate from the procurement requirements if the secretary determined that "the mission of the department would be seriously impaired." The secretary must notify Congress within one week of such a determination and include a justification for deviating from standard procurement practices.

One of the most significant provisions for government contractors would be the ability of DHS and other government agencies to use commercial item procurement practices for certain acquisitions, regardless of whether the supply or service is actually a commercial item. This has a significant practical benefit to contractors because it eliminates many of the standard, and often onerous, clauses in federal contracts.

The act also called for the centralization under DHS of homeland security-related research and development programs and efforts currently underway within other departments, including Energy, Agriculture and Transportation, thus bringing under DHS supervision a research and development portfolio of

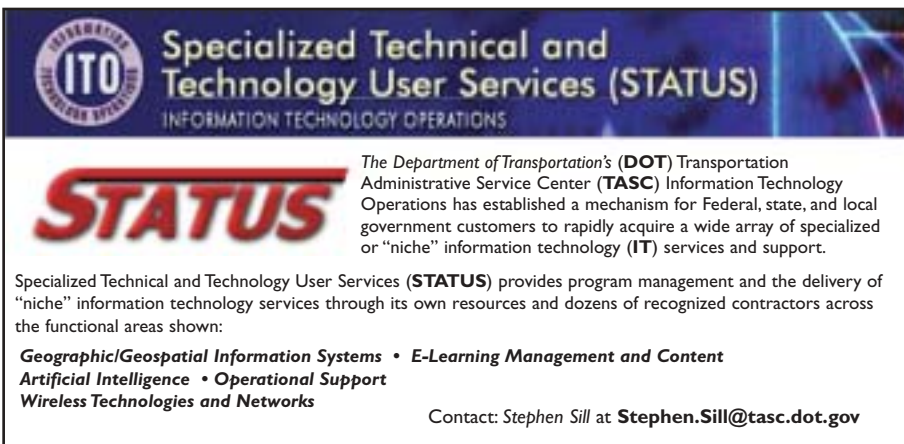
approximately \$800 million.

Congress has authorized DHS to adopt Department of Defense protocols to pursue research and development efforts through means other than contracts, grants or cooperative agreements if such traditional methods are not feasible or appropriate. DHS would be required to report to Congress annually whether such methods attract nontraditional government contractors and result in the acquisition of needed technology. The act also required revisions to the Federal Acquisition Regulation within the next year to include regulations regarding unsolicited proposals to encourage contractors to proactively provide innovative technologies to the government.

The act also provided for "Federal Emergency Procurement Flexibility," a program that would include provisions that relax acquisition requirements throughout the government for solicitations issued during a one-year period following the act's enactment. These provisions included the implementation of measures, such as increasing the threshold for the use of simplified acquisition procedures and for simplified acquisition purchases and micro-purchases. These provisions would be applicable to any agency procuring goods or services used to facilitate defense against or recovery from terrorism or nuclear, biological, chemical or radiological attack.

Additionally, the act included waivers for certain small business threshold requirements to facilitate involvement of small and minority-owned businesses in DHS procurement activities and efforts. DHS would be required to report to

continued on page 14



Specialized Technical and Technology User Services (STATUS)
INFORMATION TECHNOLOGY OPERATIONS

The Department of Transportation's (DOT) Transportation Administrative Service Center (TASC) Information Technology Operations has established a mechanism for Federal, state, and local government customers to rapidly acquire a wide array of specialized or "niche" information technology (IT) services and support.

Specialized Technical and Technology User Services (STATUS) provides program management and the delivery of "niche" information technology services through its own resources and dozens of recognized contractors across the functional areas shown:

Geographic/Geospatial Information Systems • E-Learning Management and Content
Artificial Intelligence • Operational Support
Wireless Technologies and Networks

Contact: Stephen Sill at Stephen.Sill@tasc.dot.gov

The Rules and Law of Government Appropriations

Understanding how to spend and keep federal dollars
The GAO Red Book explained in practical terms

Government Best Practices Training Conference™

Tuesday and Wednesday, February 25 and 26, 2003

Time: 7:30 AM Registration

Program Starts: 8:15 AM

Wrap-up: 4:30 PM

Course Materials, Continental Breakfast,
Refreshments, Lunch included.

Training Program will begin at 8:15 AM.

American Institute of Architects (AIA)
Building
Executive Board Room
1735 New York Avenue
Washington, D.C.

About This Course: The Rules and Law Governing Appropriations

In 1982, the GAO released its first edition of Principles of Federal Appropriations Law. It was a collection of the body of law governing the expenditure of federal funds. In 1991, the current four set volume was released.

Today, agency program managers, general counsel, contracts administrators and financial officers are all faced with significant challenges in meeting organization needs within current budgets. What are the rules? How are they applied in practice? What are the typical mistakes made that result in wasted or lost funds? How can an agency protect its budget? How can an agency manager maximize their allocation?

The rules governing federal appropriations are complex, extensive and fill four binders. This course, taught by leading experts in government contract law, will provide the student with an overview of the rules, how they are applied, and most importantly, how to maximize funds with budget limits AND within the rules.

Who Should Attend ...

- Agency Program Managers • Budget and Financial Officers • General Counsel
- Contracts Administrators • Procurement Executives • Federal support contractors
- Federal product and services suppliers, systems integrators

A detailed outline for this two-day course is available at www.marketaccess.org

Speakers:

GAO (Invited)

OMB (Invited)

James P. Gallatin, Jr.

Partner, Corporate & Securities and Government Contracts Groups
jgallatin@reedsmith.com

James P. Gallatin, Jr. has more than 24 years of experience in the area of government contracts on behalf of a wide range of public and private companies. Mr. Gallatin focuses his practice primarily on claims, litigation, bid protests, and civil/criminal investigations at the federal, state, and local government levels.

He principally represents companies in the construction, defense, and healthcare industries, and is counsel to numerous Fortune 100 corporations.

Christopher L. Risetto

Partner, Government Contracts & Export Compliance Group
crisetto@reedsmith.com

Christopher L. Risetto practices in the areas of grants and infrastructure, including environmental law, government contracting, infrastructure development and appropriations legislation. His practice emphasizes the Clean Water Act, government contracts and other environmental law, such as Superfund, the Safe Drinking Water Act, the Clean Air Act, and other public works legislation. Additionally, he counsels clients on transportation issues including the Intermodal Surface Transportation Efficiency Act of 1992 and other transportation grant programs, including the FAA.

Mr. Risetto's practice involves representation of large and small municipal clients and private corporations. His expertise includes Clean Water Act regulatory programs, including EPA construction grants audits, NPDES permit strategy, pretreatment, and enforcement defense, wetlands permitting by EPA and the Corps of Engineers, Superfund, hazardous waste cleanup contracting, and related procurement, bid protest, construction claims, suspension and debarment, legislation, and litigation. Mr. Risetto also practices in grant programs of other agencies, including the U.S. Agriculture, Commerce and Justice Departments.

Stephen M. Sorett

Counsel, Government Contracts Group
ssorett@reedsmith.com

Stephen M. Sorett is an attorney in the Washington, D.C. office of Reed Smith who focuses on all phases of government contracting with an emphasis on outsourcing, privatization, and project finance transactions. For many years he has dealt with all aspects of the public contracting process at all levels of government, and his experience includes contract formation administration, claims, and audit resolution; and in the past few years has worked extensively with companies and governments in the emerging field of electronic commerce including Business-to-Business and Business-to-Government transactions.

..other speakers to be announced.

Points of Contact:

- For information on exhibitor arrangements, please contact Ms. Cara Lombardi, 703/807-2743
- For registration or general information about this event, please contact Mr. Parrish Knight, 703/807-2748.

Registration Fee:

- Industry Credit Card or Check in Advance \$1195
- Government Credit Card or Check in Advance \$995

Go to
www.marketaccess.org
to see the TOP 10
REASONS (Plus 2) TO
ATTEND THIS
COURSE

The Homeland Security Act: Implications for Government Contractors

continued from page 12

Congress by March 31, 2004, on the use and effectiveness of the Federal Emergency Procurement Flexibility program, as well as any additional recommendations.

Liability Protections

The act provided products liability protections for providers of homeland security products and services by incorporating the Safety Act of 2002. These special liability protections – including a prohibition on the recovery of punitive damages, the limiting of noneconomic damages to situations where the plaintiff suffered physical harm, and the reduction of a plaintiff's recovery by the amount of collateral source compensation, such as recoveries from insurance and other sources – apply to qualified anti-terrorism technologies that have been certified and approved by the secretary and listed on an Approved Product List for Homeland Security.

Factors used in determining whether a technology would qualify for liability protection include, but are not limited to,

prior use and demonstrated utility and effectiveness in the defense against acts of terrorism, potential risk to the public if the technology is not deployed, liability exposure to the seller or other providers, and the risk that the technology may not be deployed absent an extension of liability protection.

The act also permitted “a rebuttable presumption that the government contractor defense applies” in products liability or other lawsuits relating to anti-terrorism technologies approved by the secretary. This presumption could be overcome only by a showing that the contractor engaged in fraud or willful misconduct in submitting information regarding the technology to the secretary during his or her consideration of the technology.

The president also signed legislation Tuesday, Nov. 26, 2002, designed to provide assistance to the insurance industry. President Bush said passage of the terrorism insurance legislation would assist in the nation's economic recovery by allowing companies to get affordable insurance for large construction projects, thereby

creating thousands of needed jobs. This legislation would require the government to provide reinsurance covering up to \$90 billion in losses during the first year of the measure's three-year term.

Freedom of Information Act Restrictions

The act expanded Exemption 4 of the Freedom of Information Act by exempting “critical infrastructure information” that is voluntarily provided to the government by a private party relating to “the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution or other informational purposes.”

This enhanced exemption is designed to promote and encourage disclosure to the government of security-related information, and to shield the disclosing party from possible competitive harm. Given the breadth of this exemption, DHS would have broad discretion to preclude information from public disclosure under FOIA.

Tac-ALERT™ 2010

Responder/Command Tactical Vest Series



- Allows for standardized stowage and retrieval of incident response gear with options for sidearm, PAPR and utility/mask carrier rigged for left or right.
- Enhanced visibility/multi-color, removable I.D. and Title panels along with reflective outlining available for positive “Who's who and who's where?”

- Federal Contract # GS-07F-0280K (Bomb Disposal & Chemical Warfare Equipment)
- See below for additional features and general information.
- Restricted sale: available to local/state/federal agencies only.

Tel: (651) 730-7000
Toll Free: (800) 777-5630
Fax: (651) 730-5680

2280 Ventura Drive St. Paul, MN 55125



<http://www.headlitescorp.com>

David Nadler is a partner in the law firm of Dickstein Shapiro Morin & Oshinsky LLP in Washington, D.C. He is an authority on federal, state and local government contract matters pertaining to the information technology industry and serves on the Homeland Defense Journal board of advisers.

Bradley Wine is an associate in the firm's technology practice group specializing in litigation and corporate counseling with an emphasis on issues affecting government contractors.

Companies have different goals.

So why settle for a 'cookie-cutter' solution?

With more than 60 years of combined industry experience, the principals of Aronson Capital Partners have a proven track record of completing successful transactions with middle-market companies. They provide a full range of corporate finance services to both buyers and sellers, helping them achieve their growth and liquidity goals.

To learn more about how Aronson Capital Partners can help you exceed your objectives, call Larry Davis today at 301.231.6225 or ldavis@aronsoncompany.com.



Securities transactions are executed by Aronson Capital Advisors, LLC (member NASD-SIPC)

Verga Clarifies DoD's Homeland Defense Role

By Gerry J. Gilmore
American Forces Press Service

In defending the homeland, the Department of Defense has clear and defined responsibilities often very much separate from those of civil organizations, a senior

Pentagon official noted Tuesday, Dec. 10.

Accordingly, the Defense Department recognizes there are differences between the homeland security and homeland defense missions, Peter Verga, director of DoD's Homeland Defense Task Force, reminded a security conference audience in Washington, D.C.

DoD supports national homeland security through its military homeland defense missions, Verga explained.

He said President Bush describes the homeland security mission as a concerted effort to prevent terrorist attacks within the United States, to reduce the nation's vulnerability to terrorism, and to minimize damage and to assist in recovery efforts after terrorist attacks.

However, Verga noted that fiscal 2004



Deputy Undersecretary of Defense (Policy Support)
Peter F. Verga

Defense Planning Guidance defines homeland defense as the military protection of U.S. territory, the domestic population and critical defense infrastructure against external threats and aggression.

The DPG also calls for DoD to routinely study state activities to deter potential aggressors and to prepare U.S. military forces for action, if needed.

"That's a subtle, but a very, very distinct difference," Verga pointed out, noting that the terms homeland security and homeland defense "are often - very incorrectly - used interchangeably."

There are three circumstances where DoD would be involved in homeland security activities within the United States, he noted. They are:

- Traditional military missions performed inside the United States, called "extraordinary circumstances." An example would be the current combat air patrols, during which military aircraft might be ordered to

shoot down a terrorist-hijacked airliner that's en route to a target.

- Emergency circumstances, where the military aids civil authorities or other federal agencies with logistical and other support in, for instance, disaster relief missions after hurricanes, tornadoes and floods.
- Temporary circumstances, such as DoD support to the Olympics.

DoD's foremost mission, Verga pointed out, is to defend the United States and the American population. Any department activities requested in support of homeland defense efforts should be centrally coordinated, he noted, to promote efficiency and prevent confusion.

The mechanisms to coordinate such DoD support are either in place or soon will be, Verga noted, citing the March 2003 start up of the Department of Homeland Security, and the authorization of a new assistant secretary of defense for homeland defense.

He also pointed to the Oct. 1 establishment of U.S. Northern Command, the new unified command with responsibility for homeland defense.

Army Lt. Gen. Joseph Kellogg, director of command, control, communications and computer systems (J-6) for the Joint Staff, sat on the discussion panel with Verga. He noted Northern Command is the first regional combatant command in the United States.

Northern Command's job, he noted, is to coordinate with other elements and agencies to produce "a seamless battlefield."

"We view the United States of America as a battlefield. If you look at what happened back on the 11th of September a year ago, ... those attacks occurred ... within the United States," Kellogg emphasized.



**Why should you use DAPS
for document management,
output, or storage?**

**50 YEARS OF EXPERIENCE
IN SECURING
DOCUMENTS FOR
THE DOD & OTHER
FEDERAL AGENCIES**



Services include:

**Document Conversion
Content/Knowledge Mgmt
CD ROM
Digital printing
Secure E-Business
Copier Management
... and much more!**

**Rest Assured . . With DAPS!
TOLL FREE 1-877-DAPS CAN
www.daps.dla.mil**

Advertise in the
Homeland Defense Journal

For more information, contact
Cara Lombardi at
(703) 807-2743 or send an
e-mail to
clombardi@homelanddefense-journal.com



Homeland Defense Journal to Survey and Profile its Readership

Effective January 1, 2003, all readers of **Homeland Defense Journal** will be requested to complete the survey form noted here. Our goal is to provide our advertisers with information about our readership and newspaper format. Your assistance will be greatly appreciated and allow us to continue to provide **Homeland Defense Journal** free to all subscribers.

The information we receive will only be used in the aggregate to profile our readership. Summary results of the survey will be reported in **Homeland Defense Journal** in early 2003.

Homeland Defense Journal

"We are 100% Homeland Defense - This is our mission, our only mission."

Homeland Defense Journal Reader Survey

Your name:

Your title:

Your company/agency or department:

City:

State:

Zip:

Email Address:

[Home](#)
[Subscribe](#)
[Advertise](#)
[Contact Us](#)

1. What is the estimated number of employees in your organization?

#:

2. Select your Industry:

3. Please select from the following list the primary areas that most reflect the mission of your organization (Select all that apply)

- ☐ Acquisition - Procurement
- ☐ Agriculture/Food Safety
- ☐ Chem - Bio - WMD
- ☐ Cyber Security
- ☐ Disaster recovery/Disaster planning
- ☐ Emergency management and Decision support
- ☐ Emergency medical - hospital - public health
- ☐ Executive information systems, command and control, decision aids
- ☐ Fire
- ☐ Geographic Info Systems (GIS)
- ☐ HAZMAT
- ☐ Incident command/Command Centers
- ☐ Information sharing and data warehousing
- ☐ Information technology
- ☐ Infrastructure protection (e.g. water, transportation, food supply)
- ☐ Mobile and Wireless
- ☐ Outfitting emergency response teams
- ☐ Physical security/Perimeter security
- ☐ Police/Public Safety
- ☐ Policy - Planning
- ☐ Program management
- ☐ R&D
- ☐ Telecommunications
- ☐ Training and simulation
- ☐ Transportation security
- ☐ Other, please identify:

4. Where do you obtain information about products and services that your organization may purchase? (Select all that apply)

- ☐ Conferences/Seminars
- ☐ Trade Shows
- ☐ Internet
- ☐ Newsletters
- ☐ Magazines/Journals/Periodicals
- ☐ Associations
- ☐ Consultants
- ☐ Internal Company Sources
- ☐ Other, please identify:

5. What type of information presented in the Homeland Defense Journal is most valuable to your organization?

6. Please identify your role in the selection of goods and services procured for your organization's use or for your clients:

- ☐ Active role in decision process
- ☐ Recommend, Provide user input.
- ☐ Technical or business management review and recommendation
- ☐ Not involved at all

7. Do you FORWARD the Homeland Defense Journal to others by email?

☐ Yes
☐ No

7a. If so, average number of people to whom you forward each issue

#:

8. Does the Homeland Defense Journal provide you with information that is useful to your mission? Do you have any comments or recommendations?

9. Would you prefer a printed copy to be mailed to you or do you prefer the pdf file that we distribute now?

☐ Yes, prefer printed copy
☐ No, prefer pdf format.

10. Do you print a copy of the Homeland Defense Journal from your computer?

☐ Yes
☐ No

Wargame Reveals Port Security Threat

At current preparedness levels, a "dirty bomb" attack through the ports could cost U.S. businesses billions

In a strategic simulation of a terror attack designed to thoroughly assess America's vulnerability through its ports, a group of business and government leaders found that such an attack could potentially cripple global trade and have a devastating impact on the nation's economy. The group focused on ways to improve detection before a weapon gets to a U.S. port, as well as help businesses to build resiliency into their operations.

The two-day Port Security Wargame, sponsored by global management and technology consulting firm Booz Allen Hamilton and The Conference Board, took place the first week in October in Washington, D.C., with 85 leaders from a range of government and industry organizations who have a critical stake in port security.

In the wargame scenario, a radioactive dirty bomb slipped through port security and was discovered when it fell off a truck at the Port of Los Angeles. A second identical dirty bomb was unpacked from a shipping container in Minneapolis, having arrived by truck via Canada. The same day, Georgia Port Authority Police Force arrested three men, one on the FBI watch list for suspected terrorists, on suspicion of attempted cargo theft.

Wargame participants from a range of government agencies, port authorities, consumer goods manufacturers, insurers, technology providers and carriers grappled with ways to balance security while maintaining an open and efficient flow of goods through U.S. supply chains. Key lessons learned included:

- Public and private partnerships are essential.

Local concerns quickly bubble up to become national and international crises. A decision to close a port completely and quickly creates issues for businesses and, ultimately, consumers. Therefore, cooperation between government and industry organizations, at both the local and national level, is critical. "The government needs to involve industry in designing their 'port security solution' so that it does not destroy businesses," noted one wargame participant.

- Port security starts at the point of origin.

A risk assessment of an individual container needs to be made before it gets to U.S. shores. The options are limited after a container has landed. Port security must be expanded to involve every link in the chain of delivering goods to market, from origin through the entire transportation system: sea, land, rail and air.

- Security must be embedded, not "bolted on." Every sector with a stake in port security — government agencies, port authorities, manufacturers, shippers, trade associations — needs to rethink its respective activities behind the act of moving inter-

national goods into the United States, and build in security to everyday processes. For businesses, this also means rethinking their supply and logistics chains, looking at changing capacity, increasing routing alternatives, and assessing their mix of domestic and off-shore production, so that they have options in the event of a disruption.

- No single solution will secure the system.

Solutions that address only one facet of port operations, such as increasing the number of containers inspected, will fall short. Securing global logistics is a complex, systemwide endeavor.

- Federal leadership needs to be unified.

"We need to overcome organizational inertia and conflicting agendas," said one wargame participant. A single government focal point must be created to effectively deter and detect terrorist events, and to oversee response, communications and ensure economic recovery.

The actions of participants had dramatic consequences:

- Decisions made by the teams led to shutting down every port in the United States for eight days
- The backlog of container deliveries caused by the closure would require 92 days to be resolved
- There would be a forecasted resulting loss of \$58 billion in revenue to the U.S. economy.

"The game revealed that port security is everyone's concern, and everyone's responsibility," said Mark Gerencser, Booz Allen Hamilton vice president. "The key to securing our ports is to maintain security throughout the whole supply chain, from the factory to the end user. The ports serve as a checkpoint, but they cannot provide a foolproof security screen. And we have seen that disruptions caused by security breaches can create enormous economic consequences."

About Stateside Associates:

Stateside Associates helps companies, industry associations and other clients work effectively with state and local governments.

Established in 1988,

Stateside is the

leading national state

and local government

relations management firm.

STATESIDE ASSOCIATES

Gaining competitive advantage and cost-saving through quality information, expert planning and execution- that is the essence of state government relations.

The firm's capabilities, depth of experience, dedication to client service and reputation for innovation in government affairs are unmatched. For more information on how Stateside Associates can help your organization, go to www.stateside.com.

Hundreds of Billions Being Spent for War on Terrorism

America spent \$137.6 billion on the war on terrorism in fiscal 2002 and is committed to spend almost double that amount — \$252.5 billion — in 2003, according to an analysis conducted by International Horizons Unlimited, a terrorism prevention and strategies think-tank based in San Antonio, Texas.

The analysis, current through November 26, 2002, was culled from public documents supplied by the General Accounting Office, the Office of Management and Budget, five federal departments and multiple agencies, state and local entities, private sector sources, and proposals for 2003 spending levels.

SUMMARY CHART: SPENDING ON THE WAR ON TERRORISM

ITEM	2001-2002	2003
Military war on terrorism including Afghanistan, Indonesia, Philippines, Yemen and Pakistan (and financial support)	\$40 billion	\$35 billion (adding Iraq)
Airline loan guarantees	\$25 billion	Unknown
Airport security	\$7 billion	Not available
Terrorism-related insurance claims, covered for 9/11/01 losses	\$40 billion	Up to \$15 billion in annual claims by insurance industry and up to \$90 billion from federal government
Department of Homeland Security	Unknown	\$80 billion, including operating budget of \$37.45 billion
Upgrading of intelligence functions	\$5 Billion	\$5 billion for FBI or other domestic intelligence agency
Rebuilding of New York City And the Pentagon	\$4.2 billion	-----
Private sector investment in security and securing the critical infrastructure	\$2 billion	\$4 billion
University and private sector research	\$1.7 Billion	\$3.9 billion
Combating cyberterrorism	\$1.5 billion	\$3 billion
First responders training, protective gear, chemical detection equipment	\$937 million	\$3.5 billion
Bio-terrorism to the Department of Health and Human Services — public health, laboratories, surveillance	\$3 billion	\$4.3 billion
Transportation and Security Administration	\$4.7 billion	\$5.3 billion
Trucking industry	\$500 million	\$500 million
State, regional and local Efforts, including law enforcement, planning, first responders and healthcare	\$2.1 billion	\$3 billion
TOTAL	\$137.6 billion	\$252.5 billion



JANUARY

Regional, State and Local Homeland Defense

Jan. 14-16
Colorado Springs, Colo.
(Includes special Grants Workshop)
www.homelanddefensejournal.com

FEBRUARY

Homeland Defense Outlook 2003

Feb. 6
Arlington, Va.
www.homelanddefensejournal.com

Disaster Conference: 24th Annual International Disaster Management Conference

Feb. 6-9
Orlando, Fla.
The Rosen Centre

Government Best Practices Training: The GAO Redbook in Practical Terms – The Rules and Law of Appropriations

Feb. 25 – 26
Washington, D.C.
www.homelanddefensejournal.com

Homeland Defense: Information Sharing

Feb. 26
Arlington, Va.
www.homelanddefensejournal.com

Government Best Practices Training: Managing Human Capital

Feb. 27
Washington, D.C.
www.homelanddefensejournal.com

MARCH

Benchmarks Conference: 6th Annual Benchmarks 2003: Creating the Efficient ED

March 6-8,
Orlando, Fla.
Renaissance Orlando Resort at Sea world
www.femf.org

Homeland Defense: Cyber Infrastructure Protection

March 11
Arlington, Va.
www.homelanddefensejournal.com

JULY

ALS/BLS Competition Bill Shearer International ALS/BLS Competitions

July 9-10
Orlando, Fla.
The Rosen Centre
www.femf.org

ClinCon Conference 2003

July 10-13
Orlando, Fla.
The Rosen Centre
www.femf.org

AUGUST

Symposium by the Sea 2003

August 23-25
Ponte Vedra, Fla.
The Sawgrass Marriott
www.femf.org

SEPTEMBER

Sand Key EMS Summit 2003

September 2003
Clearwater, Fla.
Sheraton Sand Key Resort
www.femf.org

Submit your events by sending a short description, less than 75 words, to events@homelanddefensejournal.com. Listings will run as space permits. To guarantee placement, contact Cara Lombard, clombardi@homelanddefensejournal.com.

Join our Team!!

Homeland Defense Journal

Homeland Defense Journal has an immediate opening for a full-time administrative assistant/events coordinator. Successful candidate would perform office duties; conference set-up, promotion and registration; provide telephone help and coordination with speakers, sponsors and exhibitors; help with sales efforts and database management. Familiarity with the federal market is preferred. Candidate must be self-motivated and will possess excellent verbal and written communication skills and the ability to handle multiple demands while maintaining attention to detail.

Submit resumes via e-mail to publisher –
ddickson@homelanddefensejournal.com.

Please do not send attachments – paste resumes in e-mail

Bush Orders Smallpox Shots for Military, First Responders

By Kathleen T. Rhem
American Forces Press Service

President Bush announced Friday, Dec. 13, 2002, that he has ordered smallpox vaccinations to begin for military personnel.

He also recommended medical personnel and first responders receive the vaccine, but on a voluntary basis. Administration officials stopped short of recommending widespread vaccinations of the American public.

"Men and women who could be on the frontlines of a biological attack must be protected," the president said during an afternoon press briefing in the Eisenhower Executive Office Building.

The president stressed his decision was not based on a specific threat, but on the renewed focus on security brought about by the Sept. 11, 2001, terrorist attacks and the subsequent anthrax attacks through the mail.

"To protect our citizens in the aftermath of Sept. 11, we are evaluating old threats in a new light," he said.

Smallpox is highly contagious viral disease. It is often fatal and nearly always disfiguring. There is no cure or treatment.

The eradication of smallpox as a naturally occurring disease is one of the greatest triumphs of the World Health Organization. Bush noted the risk of smallpox was so remote by 1972 the United States quit routine vaccinations.

The military continued vaccinating recruits until 1990.

A DoD release indicated the department will immunize personnel based on their occupational responsibilities, with emergency response teams and hospital and clinic workers receiving the vaccine first. Next will be those individuals with "critical mission capabilities."

The smallpox vaccine is licensed by the Food and Drug Administration and is from the same stocks used before routine vaccinations stopped in the 1970s. Though the vaccine is considered safe and effective, vaccination is not without risks. Medical officials warn that there is a slight possibility of severe reactions for some people.

Public health officials warn that certain skin disorders shouldn't receive the smallpox vaccine. pregnant women, individuals with weakened immune systems, and those with

continued on page 21

Homeland Head, Health Care Pros Outline President's Smallpox Plan

By Sgt. 1st Class Doug Sample
American Forces Press Service

Homeland Security Adviser Tom Ridge said today the strategy for the president's smallpox vaccination plan is to immunize frontline troops who serve in high-threat areas and domestic emergency responders.

Ridge spoke at a briefing in the Eisenhower Executive Office Building following President Bush's announcement of his plan to protect Americans in the event of a bioterrorist attack.

Joining him to help explain the different aspects of the plan were Tommy Thompson, secretary of the Department of Health and Human Services; Dr. Julie Gerberding, director of the Centers for Disease Control and Prevention; Dr. William Winkenwerder, assistant secretary of defense for health affairs; and other top federal health officials.

Ridge said the president's smallpox plan was brought about after the terrorist attacks of Sept. 11 revealed the nation's need for a better security plan, and brought to light the nation's vulnerability to a terrorist attack.

"Clearly from Day 1, we've been concerned about weapons of mass destruction ... and one of the highest priorities involved smallpox because of its destructive consequences as an agent. It's one of the agents that any country should fear," Ridge said.

Thompson said he is working with state and local governments to draft plans to create smallpox response teams made up of volunteer emergency health and medical personnel. He called the teams critical to the plan to provide critical care and services immediately following a smallpox attack. He said the vaccine and the vaccinations would be made available on a voluntary basis to team members.

"This program centers on these smallpox response teams and first responders for a strategic reason," Thompson said. "Since a smallpox release is possible, we must prepare by offering to those most likely needed to respond. By preparing our emergency responders, we are better able to protect the American people, and this has to our highest priority."

He said the initial stage of the program, which has been in the planning stage for the past year, will not be offered to the general public at this time, even though the United States has enough vaccine to immunize every person in the country. Thompson did say the government would take measures to accommodate citizens who want to have the vaccination done now.

Ridge underscored Bush's comments regarding the existence of an imminent threat of a smallpox attack against the American public. There isn't one, he acknowledged, but the possibilities are real.

"There is no intelligence that talks about an imminent threat of a biological weapon involving smallpox, but because of the nature of that agent and what it could do, we knew we had to come up with a national strategy, a national plan," he said.

In his announcement, the president said a big part of the national plan will include some 500,000 military, who he has ordered to receive mandatory smallpox vaccinations.

Winkenwerder confirmed that the military vaccination program is under way. He told reporters that a "few soldiers" at nearby Walter Reed Army Medical Center had already received the smallpox vaccine. He described the soldiers as members of a military emergency medical team, but declined to identify them or detail the military's plans.

Bush Orders Smallpox Shots for Military, First Responders

continued from page 20

Bush said he'd be vaccinated because he wouldn't order military personnel to take anything he wasn't willing to take himself. However, he added, his family and staff would not be getting the vaccines because public health and national security experts are not recommending them for the general public.

"These vaccinations are a precaution only and not a response to any information concerning imminent danger," Bush said. "Given the current level of the threat, and the inherent health risks of the vaccine, we have decided not to initiate a

broader vaccination program for all Americans at this time."

The president noted that the cautionary vaccinations are a necessary step to guard against possible threats to the nation. "It is prudent to prepare for the possibility that terrorists who kill indiscriminately would use disease as a weapon," he said.



White House photo by Paul Morse

President George W. Bush discusses his smallpox vaccination program during a press conference as Secretary of Health and Human Services Tommy Thompson, left, and Director of the Office of Homeland Security Tom Ridge in the Dwight D. Eisenhower Executive Office Building Friday, Dec. 13.

Advertise in the **Homeland Defense Journal**

For more information, contact
Cara Lombardi at
(703) 807-2743 or send an
e-mail to

clombardi@homelanddefensejournal.com



Not business as usual - but business as it should be.

Today's industry leaders describe their success strategies for surviving and thriving in uncharted waters. Don't miss the unique value in the industry's fastest growing conference & exhibition.

- **Evaluate** all wireless broadband technologies under one roof
- **Discover** winning solutions available NOW in license exempt and licensed spectrum bands
- **Review** products and services from more than 40 exhibitors
- **Network** with 1,000+ colleagues from 20 nations
- **Attend** collocated meetings of the License Exempt Alliance, IEEE 802.16, FSO Alliance, TDD Coalition and many other supporting industry associations

Fairmont Hotel • San Jose, CA

January **13-15**
2003

Attend the World's Premier
Technical Event On Wireless Broadband

WCA's 9th Annual Technical Symposium & Business Expo

New format in 2003 includes jury selected papers, operator success stories and targeted forums on NLOS, wireless security, 802.11, license exempt solutions, rural MDS deployments, new rules—and more!

For more information or to register visit

www.wcai.com or call **1.202.452.7823**

Rising to the
CHALLENGE in
Broadband



DoD Looks Forward to Working With Homeland Security Department

By Jim Garamone
American Forces Press Service

The Defense Department looks forward to helping the new Department of Homeland Security in any way it can, said Peter Verga, director of DoD's Homeland Defense Task Force.

Verga said DoD would cooperate with the new agency even as it establishes the new position of assistant secretary of defense for homeland defense. Congress authorized the new position in the 2003 National Defense Authorization Act.

He said DoD is anxious to begin working with the Department of Homeland Security. "We think the consolidation of the 22 departments and agencies will improve the effectiveness and efficiency of how we're accomplishing homeland security," he said. The new agency should make it easier for DoD to coordinate its homeland defense and civil support activities.

The new department will have about 170,000 workers, but few are scheduled to transfer from DoD, he said. The National Communications System would transfer, as would a small chemical-biological defense research project.

The National Communications System is a consortium of private industry telecommunications companies that provides communications during a national emergency. DoD is the executive agent for system and about 90 people will transfer into homeland security.

The chemical-biological project is just starting. Only the portion having clear applicability to protecting the civilian population will transfer, Verga said, and at this point it is too early to say how many workers will be affected.

Verga said he is trying for a "seamless transition" between his office and the new Office of the Assistant Secretary of Defense for Homeland Defense. The new organization will come under the defense undersecretary for policy.

He said the new assistant secretary would have a close working relationship with U.S. Northern Command, the new unified command with responsibility for defense of the homeland. The position is not, he stressed, in the chain of command. That runs from the president to the defense secretary to the commander of Northern Command. Yet, the new assistant secretary will provide policy guidance for the command through the defense secretary, he said.

The establishment of the new office will not mean a growth in the overall size of the Office of the Secretary of Defense. Some of Verga's task force members will join the new office's staff as will some employees currently working elsewhere in the policy branch. He estimates the new office may have around 40 people.

The future of the director of military support is another aspect of homeland defense that still must be worked out. The director — currently the Army secretary — serves as the DoD contact for support to civil authorities in emergencies. This responsibility is one that is being considered for transfer to the new assistant secretary.

Verga said one of the things he has tried to do for the past year is "to work myself out of a job." The permanent organization within DoD to handle homeland defense matters will do that.

The White House will nominate the new assistant secretary sometime after the new Congress meets in January.

Transportation Security Mission Is 'Far From Over,' Agency Head Says

By Gerry J. Gilmore
American Forces Press Service

The year-old Transportation Security Administration first focused on making the skies safer for the American public after the Sept. 11, 2001, terrorist attacks, but much more needs to be done, the agency's acting director said in Washington, D.C., Monday, Dec. 9, 2002.

The now 50,000-member TSA is soon to be "intertwined" with 22 other agencies with the March 1, 2003, start-up of the Department of Homeland Security. It will continue to protect the nation's air transportation system, ports, railways and buslines, retired Coast Guard Adm. James M. Loy, TSA director, said to a homeland security conference audience here.

Loy, undersecretary of transportation for security and a former Coast Guard commandant, noted that TSA would fall under the Homeland Security Department's border and transportation security section. With more than 150,000 employees, the section would comprise the largest portion of the department's 170,000 total employees, he pointed out. TSA has achieved much in a year, Loy noted. In the days and weeks after Sept. 11, he remarked, TSA received a priority mandate from Transportation Secretary Norman Mineta to safeguard commercial aviation's 429 airports and associated operations.

On Nov. 19, he said, 40,000 highly trained federal baggage screeners replaced contract screeners previously

used at the nation's airports. And, he added, come Dec. 31, all baggage carried aboard commercial aircraft will be screened for explosive devices.

That, he remarked, represents "amazing progress" in such a short period of time.

However, he emphasized that TSA's achievements will continue into the future, promising "continuous improvement" of the agency's security systems and administrative operations as it becomes a part of DHS.

"Please challenge us ... to do things better," he told his audience, adding that if improvements to the nation's transportation security systems aren't made, then "the bad guys" will take advantage of it.

continued on page 24

Colorado Springs, Colorado
Photos supplied by the
Colorado Springs Convention
and Visitors Bureau

Homeland Defense and Homeland Security

in the 21st Century

Regional, State and Local Strategies

Homeland Defense Training
Conference TM
Colorado Springs, Colorado

Three-day Training Conference
and Grants Workshop
Tuesday – Wednesday –
Thursday
January 14, 15, 16, 2003
Broadmoor Conference Resort
Colorado Springs, Colorado

This conference will examine the development of strategies, requirements, solutions and plans at the regional, state and local levels. Federal agency support programs will also be examined. Other topics include:

- Report on federal and state grants to support homeland defense initiatives
- Grants workshop with tips, tools, lessons-learned
- Briefings by Northern Command on roles, mission and requirements
- Report from Capitol Hill on pending legislation, funding and new programs
- Federal agency reports on roles at regional, state and local levels

Speakers Include:

- Rear Admiral Stone, J4 Logistics, NORTHCOM (Equipment supply requirements)
- Dr. Ron Sega, Director, Department of Defense - Defense Research & Engineering (DDR&E) (invited)
- Charles Benight, Colorado University

- Jeff Goldberg, EMT-P, Emergency Management Advisor to the Director of Integrated Support Services, Library of Congress
- Eric Mason, Supervisory Special Agent, CALEA Implementation Section, FBI
- William E. Ayen, Ph.D., Director, Network, Information, and Space Security Center (NISSC), University of Colorado

- Robert E. Roberts, Regional Administrator, EPA
- Valerie McNevin, State of Colorado Office of CIO for Info Security
- Lt. Frederick Hoon, Commander, 8th Weapons of Mass Destruction – Civil Support Team (WMD/CST)
- Speaker TBD, Colorado Department of Public Safety
- Speaker TBD, Joint Interoperability Test Command (JITC) DOD (Invited)

Grants Workshop Speakers:

- Stephen M. Sorett, Attorney at Law, Reed Smith, Washington, D.C. (Nationally recognized Grants law expert)
- Christopher L. Rissetto, Partner, Reed Smith, Washington, D.C. (Nationally recognized Grants law expert)
- Michael Paddock, President, Grants Office LLC (Mr. Paddock will chair the Grants Workshop)
- FEMA – First Responder Grants (Name to be provided)

Who Should Attend

- Regional, state and local emergency management executives and senior staff
- Federal and DoD managers with an assigned mission in homeland defense
- Industry executives with products and services that support homeland defense
- Trainers and instructors in emergency response
- State and local grants staff interested in updating their understanding of available grants and grants application techniques

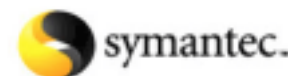
SPONSORS:



University of Colorado



ReedSmith



Special Exhibit and Sponsor Opportunities Available.

Call Cara Lombardi at 703-807-2743 for more information or clombardi@marketaccess.org.

For more information, registration and current list of speakers, go to www.homelanddefensejournal.com.

Transportation Security Mission Is 'Far From Over,' Agency Head Says

continued from page 22

Loy looks forward to securing better airport screening equipment and to enrolling passengers who fly frequently in a voluntary identification system program. Frequent fliers who sign up would clear security more quickly, he said.

Also, Loy envisions that pilots, mechanics, drivers, maritime dockworkers, and ships' crews would eventually

undergo special security checks and receive biometric credentialing (iris scans, fingerprint checks) in order to access the nation's airports and ports.

Efficiency gained from such a system means credentialed persons could be issued just one ID card, rather than the up to the 23 IDs now provided to some transportation employees in critical security

positions, he said.

Loy maintained the bottom line is, it's more than appropriate to improve the nation's internal security system for the next generation of Americans.

"There is no more important work being done," he concluded.

Civil Air Patrol and FAA: Drug Trafficking and Terrorism Are Connected

By John Kittle

For Homeland Defense Journal

Investigations have established a definite tie between global illegal drug trafficking and terrorism, according to experts at the Fall 2002 Anti-Smuggling Investigators Association (ASIA) in Atlanta, Ga.

The conference, co-hosted by the Civil Air Patrol (CAP) and the Federal Aviation Administration (FAA), was intended to promote the free exchange and dissemination of intelligence and best practices pertaining to smuggling and illegal drug trafficking. Its scope includes all phases of smuggling via air, land and sea. Since the terrorist attacks September 11, 2001, ASIA has broadened its scope to include counterterrorism and homeland security.

"CAP can be a big help in the fight against smuggling, terrorist activities and weapons of mass destruction," said Al Allenback, CAP executive director. "The marriage of low-cost aerial platforms with leading-edge imaging and sensor technology gives CAP a unique capability to deliver cost-effective reconnaissance. CAP is a force multiplier for your operations and a great value for the tax-

payers. CAP can put an airborne platform over any major metropolitan area or strategic resource in the United States in two hours or less for \$90 an hour."

Scott Burns, deputy director for the Office of State and Local Affairs, Office of National Drug Control Policy (ONDCP), was the keynote speaker for the conference. Within the Executive Office of the President, the Office of State and Local Affairs is responsible for strategy, analysis and the formulation of domestic drug policy. Burns oversees national coordination and cooperation among federal, state and local counterdrug programs, including the \$226 million High Intensity Drug Trafficking Area program.

"There are 16 million drug users in the United States and 70 percent of drug users use marijuana," Burns said. "We have to address the nation's obsession with using marijuana."

Marijuana is one of the drugs ONDCP is concentrating on to achieve the President's drug-reduction goals. Burns showed several TV ad clips that are part of ONDCP's educational campaign to show America's youth the link between illegal drugs and terrorist activities.

"Ninety percent of law enforcement

is accomplished at the state and local levels," said Burns. "There has to be a coordinated effort to bring state and local law enforcement together with federal law enforcement."

John Kittle is chief, counterdrug and homeland security, for Headquarters CAP. His office is in Washington, D.C. His e-mail address is kittlej@hoffman.army.mil.



Disaster Recovery Institute International's world-renowned professional certification program (ABCP, CBCP, MBCP) acknowledges an individual's effort to achieve a professional level of competence in the industry.

Designed to be rigorous, well controlled, and free of bias, the program is centered on the Professional Practices, our international industry standard. The certification process delivers authoritative recognition of your level of industry knowledge and capabilities.

For more information about Disaster Recovery Institute Certification programs, go to **www.drii.org**.

Advertise in the
Homeland Defense Journal

For more information, contact Cara Lombardi at
(703) 807-2743 or send an
e-mail to
clombardi@homelanddefensejournal.com



FACES *In the Crowd*

Bush Names Deputy Counsel and Deputy Assistant

President George W. Bush named David G. Leitch Deputy Counsel and Deputy Assistant to the President.

Previously, Leitch worked for the Federal Aviation Administration as the chief counsel. More recently, he was detailed to the Office of Management and Budget where he served as the counsel to the Transition Planning Office for the Department of Homeland Security.



BAE SYSTEMS North America Picks Richard Ashooh

BAE Systems North America appointed Richard Ashooh vice president of legislative affairs. In this newly created position, Ashooh would provide guidance, policy direction, management and oversight of the legislative function and would represent the company for federal, state and local government affairs.



Israeli Defense Force officer Joins AMU

A former Israeli Defense Force officer, engineer and founder of an international consulting architect-engineer firm specializing in the design of protective structures and systems capable of withstanding various weapons effects, has joined the faculty of American Military University.

Reuben Eytan, the president and chief engineer of Eytan Building Design of Tel Aviv, will be teaching a new course he developed for AMU titled "Commercial Risk Mitigation."

The course is designed for the non-engineer, corporate or government officials who are responsible for controlling loss through the enhancement and/or design of threat resistant facilities, training, or the integration of insurance coverage to complement defensive risk management strategies. The course will begin in February 2003.

Eytan is an expert in evaluating commercial loss, including processes that measure damage to facilities and equipment, and the impact of business interruption, as well as personnel injury and death. He has also designed facilities to meet a wide spectrum of threats, including bomb/blast, cyber threat, and chemical/biological threats arising from terrorist or military forces.

Navy CIO Retires, Joins Vredenburg

Dan Porter, Navy chief information office, retired Sunday, Dec. 1, 2002, then joined Reston, Va.-based Vredenburg as senior vice president for strategic development.

In his new position, Porter would lead the company in broadening its presence in key markets, including homeland security, acquisition management, information management and IT solutions.



Motorola Names New President and CEO of Commercial, Government and Industrial Solutions Sector

Greg Brown was named executive vice president of Motorola and president and CEO of Motorola's Commercial, Government and Industrial Solutions Sector (CGISS).

Previously, Brown was chairman and chief executive officer of Micromuse, a provider of service and business assurance software.



Let us know about your organization's personnel changes.

Send an e-mail to

faces@homelanddefensejournal.com

Homeland Defense Business Opportunities

By Kelly Kingsley - Homeland Defense Journal

Homeland Defense Journal tapped into the database of its partner, Market*Access International, to compile this list of homeland defense opportunities and recent contract awards.

Project	Anti-Terrorism/ Force Protection Design	Defense Integration and Management of Nuclear Data Services	Work Analyst Station
Department	Department of the Navy	Department of Defense	Department of Defense
Agency	Naval Facilities Engineering Command	Defense Threat Reduction Agency	Defense Information Systems Agency
Summary	The work associated with this indefinite quantity contract for miscellaneous anti-terrorism/force protection design with associated multi-disciplinal architectural and engineering support services includes various studies, master plans and the preparation of construction documents via traditional and alternative documentation methods, (such as design-bid-build plans and specifications and design-build), ready for bidding for various projects at various locations throughout the continental United States with emphasis in the Engineering Field Activity Chesapeake Region District of Columbia, Virginia and Maryland.	The Defense Threat Reduction Agency is seeking sources to combine two legacy systems, such as the Nuclear Management Information System and Special Weapons Information Management System, into an integrated system, Defense Integration and Management of Nuclear Data Services for managing the nuclear stockpile by developing an automated end-to-end information infrastructure.	The Defense Information Systems Agency intends to award individual contracts to three vendors to obtain a product and support services to enable DISA to identify the off-the-shelf analyst workstation in the marketplace that best meets DISA's Department of Defense Computer Emergency Response Team (DoD CERT) and Regional CERT's (RCERT) operational needs. The DoD CERT and the RCERTs perform correlation and analysis of information assurance (IA) sensor data to support IA and computer network defense decision making.
Schedule	Responses due Monday, Jan.13, 2003	Responses due Wednesday, Jan. 15, 2003	Responses due Monday, Jan. 6, 2003
Agency Contact	Terrence Gragg (202) 685-1045 graggtp@efaches.navfac.navy.mil	Allen Reed (703) 325-5029 allen.reed@dtra.mil	Barbara Janitis (703) 681-0754 janitisb@ncr.disa.mil

Let us know about your company's recent contract awards. Send contract award announcements to wins@homelanddefensejournal.com.

Business Briefs

Space Imaging Opens Office in Virginia

Denver-based Space Imaging opened a federal sales office in Reston, Va. The new office would house a sales team focused on federal and civil business development, military programs and intelligence and homeland security applications.

Northrop Grumman Shareholders Approve Merger with TRW

Northrop Grumman Corp., Los Angeles, announced the preliminary vote tally from a special meeting of shareholders, affirming the company's proposal to issue approximately 70 million shares of its common stock in connection with the acquisition of TRW, Inc.

The preliminary vote tally, prepared by the independent inspectors of election, shows that approximately 89,042,870 shares, or more than 90 percent of shares voted, voted in favor of the stock issuance.

Earlier, TRW shareholders voted to approve TRW's merger with Northrop Grumman. With all regulatory and shareholder approvals now behind the companies, Northrop Grumman expects to close the transaction promptly.

Based on the exchange ratio for the merger, TRW shareholders would receive 0.5357 shares of Northrop Grumman common stock for each share of TRW common stock, with cash paid in lieu of any fractional share of Northrop Grumman stock that otherwise would be issued to TRW shareholders.

On Tuesday, Northrop Grumman entered into a consent decree with the U.S. Department of Justice that allowed the company's acquisition of TRW to close promptly after approval of the transaction by shareholders of both companies.

ClearForest Opens in Washington, D.C.

ClearForest, a New York-based company that transforms unstructured content into business intelligence and insight, opened a sales office in Washington, D.C., to support increasing demand from governmental organizations for unstructured data management tools used for counter-intelligence and other critical homeland security activities.

Rainbow Technologies Wins Orders to Secure Homeland Security Communications

Rainbow Technologies, Inc., of Irvine, Calif., announced that its Mykotronx subsidiary received nearly \$3 million in new orders for high-assurance cryptographic products. These products would be used to secure communication channels between first responders in key installations, including all U.S. state and territory capitols and the Office of Homeland Security in Washington, D.C.

Orders for the high-assurance products originated under several multi-year indefinite delivery, indefinite quantity contracts.

CSC to Acquire DynCorp

Computer Sciences Corp., of El Segundo, Calif., set plans to acquire Reston, Va.-based DynCorp.

The transaction is valued at approximately \$950 million, including the assumption of all of DynCorp's debt, which was \$273 million of principal amount on Sept. 26, 2002. Upon consummation of the merger, each DynCorp share would be converted into \$15 in cash and

\$43 in market value of CSC shares.

The transaction would require approval by the holders of a majority of the approximately 11 million outstanding DynCorp shares as of Sept. 26, 2002, and is subject to customary conditions, including expiration of the waiting period under the Hart-Scott-Rodino Antitrust Improvements Act.

The terms of the acquisition have been approved unanimously by the boards of directors of both companies.

CSC expects to conclude the transaction during the first calendar quarter of 2003.

Advanced AV Launches Federal Government Business Unit

Advanced AV, West Chester, Pa., formed a new business unit to provide the federal government with design, installation and technical management of intelligent command and control facilities, collaborative multi-function conference rooms and comprehensive security system monitoring.

This business unit would be called Advanced AV Federal Solutions Group and is located in Washington, D.C.

Versar Awarded \$6.5 Million Navy Contract

The Navy awarded Versar, Inc., of Springfield, Va., a contract valued at more than \$6.5 million. Initial work under the five-year contract would support the integration of network-centric data management systems at military test and training ranges in the United States.

The Navy work would integrate current range data on training, operations,

continued on page 28

Grow
your federal IT business
Develop
your federal pipeline

INPUT

For a Free Trial visit
<http://www.input.com/gov>

Empower your federal sales and business development learn with the industry's most advanced on-line database of federal IT contract opportunities, agency analysis and market assessments.

<http://www.input.com/gov>



Business Briefs

continued from page 27

research and development, readiness, budgeting and environmental planning for the development and utilization of future strategic operational Navy and Air Force range requirements.

Innolog Creates Homeland Security Division

McLean, Va.-based Innovative Logistics Techniques, Inc., an integrator of logistics systems for homeland security, defense and state and local government agencies, formed a homeland security operations division.

The company plans to leverage its role in deploying and training more than 44,000 passenger screeners as one of the subcontractors on the Transportation Security Administration's Strategic Airport Security Rollout (SASR) contract to qualify for upcoming logistics management, supply chain security and other IT opportunities from the new Department of Homeland Security and the DoD.

Anteon Wins Two Contracts to Support Air Force Research Lab

The U.S. Air Force Research Laboratory, located in Dayton, Ohio, awarded Fairfax, Va.-based Anteon International Corp., two task orders with a total potential value of \$10 million.

Under a three-year task order, Anteon would provide technology services and

program management support for the AFRL Transformation Management for accelerated Technology Transition program. Under this program, AFRL teams would use improved program management methods to bring new technologies more rapidly to production for weapon systems. This program would support activities throughout AFRL and Air Force System Program Offices that are not part of the AFRL. If all options are exercised, this contract has a potential value to Anteon of \$8.8 million.

Under a 14-month task order valued at \$1.3 million, Anteon would support AFRL's Materials and Manufacturing Directorate. The Anteon team would provide advanced material research for laser protection materials as applied to designated Air Force systems using the government-owned, contractor-operated Laser Hardened Materials Evaluation Laboratory facility.

Let us know about your company's recent contract awards. Send contract award announcements to wins@homelanddefensejournal.com.

Join SAME TODAY!

The Society of American Military Engineers

We are a unique association of nearly 25,000 architects, engineers and construction officials in governments and industry throughout the United States and abroad.

SAME provides several special annual and periodic forums, education and training opportunities, and two publications devoted to new and emerging information about infrastructure security, information security, contracting, design and engineering projects, environmental issues, regulatory matters, small and large business practices, and designing and engineering technologies.

Here are just some of the benefits of membership:

- **Participation in The Infrastructure Security Partnership (TISP)** — join federal and private-sector officials to improve the security of our nation's infrastructure and our nation's capability to respond to disasters.
- **"Federal Construction, Design & Environmental Programs"** for the next Fiscal Year — the most comprehensive project-specific information available, in advance of design completion or project start, with listings of contracting officials, on CD-ROM. Free to Corporate and Public Agency members.
- **Online and Print Directories** — business data and engineering capabilities in profile form. Free profile and Web site logo for Corporate and Public Agency members. Join today's nearly 2,500 member companies and public agencies in these directories.



To join The Society, go online to www.same.org/same_mbr.htm, or contact: SAME Membership Department,

607 Prince Street, Alexandria, VA 22314-3117 Phone: (800) 336-3097 Fax: (703) 548-1463 e-mail: same@same.org